UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF: KIK USERNAME "whatthefckk" THAT IS STORED AT PREMISES CONTROLLED BY MEDIALAB, INC.	)	No. 1:21-MJ- 96-01-AJ
	)	**Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Adam Rayho, a Task Force Officer with the United States Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for content and records associated with a certain Kik user account that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a social networking company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab to disclose to the government records and other information in its possession (including the content of communications) pertaining to the subscriber or users associated with the Kik username "whatthefckk" (hereinafter referred to as the "SUBJECT ACCOUNT"), which are stored at the premises owned, maintained, controlled, or operated by MediaLab, Inc. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

AGENT BACKGROUND

2. I am a detective with the Nashua, New Hampshire Police Department, and a deputized task force officer (TFO) for HSI. I became a certified police officer in the State of New Hampshire in May 2014 after graduating from the 164th New Hampshire Police Standards and Training Academy. I have also completed HSI's Task Force Officer Course. I hold a bachelor's degree in criminal justice, with a minor in Computer Science and Victimology, from Endicott College.

3. Since November 2019, I have been assigned to the Special Investigations Division as a member to the New Hampshire Internet Crimes Against Children (ICAC) Task Force, which includes numerous federal, state, and local law enforcement agencies conducting proactive and reactive investigations involving online child exploitation. As a TFO, I am authorized to investigate violations of federal laws and to execute warrants issued under the authority of the United States. Specifically, as a TFO and a member of the ICAC, I investigate criminal violations related to online sexual exploitation of children. I have received training in the areas of child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual activity, by attending training hosted by the ICAC involving online undercover chat investigations and interview/interrogation. I have also participated in numerous online trainings hosted by the Federal Bureau of Investigation Child Exploitation and Human Trafficking Task Force Online Covert Employee Development Series. These trainings focused on live stream investigations, using undercover personas on various social media applications for proactive investigations, including on Kik Messenger. In addition, I have completed the Cellebrite Certified Operator and Cellebrite Certified Physical Analyst course in mobile forensics. In the course of investigating crimes related

to the sexual exploitation of children, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous online child sexual exploitation investigations and am very familiar with the tactics used by child pornography offenders who collect child pornographic material and those who seek to exploit children.

4. Over the course of this investigation, I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, publicly-available information regarding Kik services, and information gained through my training and experience. I have set forth only the facts that I believe are necessary to establish probable cause that the SUBJECT ACCOUNT has been used to violate 18 U.S.C. §§ 2251(a), 2252A(a)(2), and 2252(a)(4)(B). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes, as further described in Attachment B.

STATUTORY AUTHORITY

5. This application is part of an investigation into Anthony Rimas and others for violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2), and 2252(a)(4)(B). 18 U.S.C. § 2251(a) prohibits a person from knowingly employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct,

including the production of child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly distributing any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252(a)(4)(B) prohibits a person from knowingly possessing any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

BACKGROUND ON KIK SERVICES

7. Through training and experience, as well as my review of Kik's guide for law enforcement and publicly available information, I know that Kik Messenger is a free social networking service owned by MediaLab, Inc., which is headquartered in Santa Monica, California. Through the Kik Messenger application, Kik users can share text messages and other content, including videos and images. Kik users can create groups for communication or sending pictures and videos; they can also exchange private messages, photographs, and videos directly with individual Kik users. Kik users and groups are identified on the Kik app by whatever user name and/or screen name they choose.

8. The Kik application is primarily used on mobile or "smart" devices, such as an Apple iPhone, Android cell phone, Apple iPad, or Android tablet. Although Kik is a platform for mobile devices, there are ways that it can be used on desktop or laptop computers. In order to do so, a person would have to install on the computer what is known as an "emulator," a program that emulates a mobile device environment.

9. Kik allows users to create a profile using a name and an email address. The email address is not verified by Kik. Additionally, Kik does not require a phone number for registration. While on Kik, Kik users can only see other Kik members' display name, user name, and profile picture, which are all chosen by the Kik user.

10. Kik exchanges are called chats, whether they are conducted by text message or video. Kik Messenger allows for group chats with up to 50 participants. The platform also facilitates real-time video chat options for live one-on-one video chat or private group video chats of up to six participants. Chats on Kik Messenger are not viewable remotely. Chats are only viewable through use of a Kik user's password and on the device where the user has the application installed.

11. Kik messenger allows individuals to created public or private groups on their server which allows for multiple individuals to communicate and share files. Individuals within the group are also able to privately message other individuals within the group. The creator of the Kik group is called an owner. Through my training and experience, I know that the owner of a Kik group is either the individual who made the group or the longest active member after the original owner left the group. The owner of the group can make members of the group administrators which gives them the same privileges as the owner, such as adding individuals and removing them.

12. I am aware that Kik chats can be saved by the user in a variety of ways, including by taking screen shots using the mobile device on which Kik is used. However, once the screen shot has been created, it can easily be shared, saved, or transferred from the mobile device to any other electronic device through email, Bluetooth, or by saving the image to a removable SD card that can then be used to transfer the screen shot to the receiving device.

13. Kik collects information from and about users of the Kik Messenger application, including personally identifiable information, profile information, message content, conversation attributes, Kik communications, log and data usage information, device information, location information, and local storage information.

PROBABLE CAUSE

14. As a Detective in the Special Investigations Division working with the Internet Crimes against Children (ICAC) Task Force, I maintain several online undercover ("UC") profiles, used in proactive investigations regarding the exploitation of children on the internet. The online undercover persona used during this investigation, was that of a 14-year-old female. During this investigation I spoke with a male later identified as Anthony Rimas ("RIMAS") via the applications Whisper,[1] WhatsApp,[2] and Zoom.[3] During conversations with RIMAS on these platforms, he solicited who he thought was a 14-year-old female to engage in sexual activity. In

[1] Whisper is a proprietary Android and iOS mobile app available for free download. It is a form of anonymous social media, allowing users to post and share photo and video messages anonymously.

[2] WhatsApp Messenger, or simply WhatsApp, is an American freeware, cross-platform centralized messaging and voice-over-IP service owned by Facebook, Inc. It allows users to send text messages and voice messages, make voice and video calls, and share images, documents, user locations, and other content.

[3] Zoom Video Communications, Inc., aka Zoom, is an American communications technology company which provides video, telephone, and online chat services through a cloud-based peer-to-peer software platform.

addition, he requested that the 14-year-old take photos or videos of herself engaging in sexually explicit conduct. I completed state search warrants for the phone number RIMAS was using for the WhatsApp application and the Zoom Meeting ID RIMAS used for Zoom calls. The results of the search warrants produced several Comcast and Verizon IP Addresses which were used to access the applications. Homeland Security Investigations issued summonses to Comcast to obtain subscriber information for the IP Addresses which all resolved back to 4 Janet Lane, Newton, New Hampshire. Homeland Security Investigations also issued summonses to Verizon to obtain subscriber information for the IP Addresses which all resolved back to the phone number (978) 430-0748 which was learned to be associated with Anthony RIMAS of 4 Janet Lane, Newton, New Hampshire.

15. Furthermore, on February 1, 2021, while searching for child exploitation groups on Kik messenger I observed a group titled NH D.aughters with the unique username #nhdau.ghterfantasy. Through my training and experience I recognized this group name could be associated with the exploitation of children. Using an undercover Kik account and the persona of an adult male I joined the group. Between February 1, 2021, and continuing through the beginning of March 2021, I observed several conversations within the group and have had private conversations with members of the group which showed the majority of the members join or use the group to discuss the sexual exploitation of children. One specific example is the user "jon240c." jon240c joined the group on February 16, 2021, and was a member until February 20, 2021. The user jon240c was identified by Detective J.B. Reid of the Boone North Carolina Police Department and North Carolina ICAC/Homeland Security Investigations as an individual producing child sexual abuse material involving his three year old daughter. On February 20, 2021, I along with members of Homeland Security Investigations and the ICAC Task Force, executed a search warrant on a person named

Kyle Amaral ("AMARAL")'s residence in Ossipee, New Hampshire. Investigators confirmed AMARAL was the user of the jon24oc account and placed him under arrest. On March 29, 2021 AMARAL was indicted by a Federal Grand Jury in the District of New Hampshire for two counts of Distribution of Child Pornography and one count of Sexual Exploitation of a Minor based on his conduct in the Kik chat group and evidence uncovered during the search warrant.

16. On February 13, 2021, using an additional undercover Kik account and the persona of a 14-year-old female, I briefly joined the Kik group NH D.aughters with the unique username #nhdau.ghterfantasy. Almost immediately after joining, I received a message from the KIK user " JJ" with the unique username "whatthefckk." This user is listed as the owner of the Kik group NH D.aughters/#nhdau.ghterfantasy. The current rank structure of theKik group #nhdau.ghterfantasy lists the owner as "JJ" unique username "whatthefckk" and administrator as "Jack Daniels" unique username "jackdan8578."

17. Starting on February 24, 2021, I communicated with Kik user whatthefckk via the private message feature. During my initial conversation, I informed Kik user whatthefckk I was a 14-year-old female and he proceeded to ask questions and make statements such as "have you fucked an older man before…its time you did then." Kik user whatthefckk asked what had prompted me to join the group and I advised that my friend had dared me. Kik user whatthefckk proceeded to ask if my friend and I would join a group chat with him. I gave Kik user whatthefckk the undercover Kik username of Detective Aaron Wojtkowski (Newbury MA Police Department), who uses the persona of a 13-year-old female, and Kik user whatthefckk created a group chat involving the three of us titled "Jenni's chat."

18. From February 24, 2021, to March 04, 2021, Detective Wojtkowski and I communicated with Kik user whatthefckk in the group chat. During the group conversation, Kik user whatthefckk asked questions like "who want to loose their virginity" and told the UCs, that he wanted to "get you naked and play" and that he wanted to have sex with them. He later told the UC that he would like to see pictures of her vagina.

19. Furthermore, on Friday March 5, 2021, Kik user whatthefckk provided Detective Wojtkowski with the number (978) 330-6022 to contact him. This is the same WhatsApp number I previously associated with RIMAS.

20. As a result of this ongoing investigation, On March 4, 2021 I completed a preservation request for the KIK user whatthefckk. I uploaded the request via KIK's law enforcement portal and later received a response advising the reference number for my request was 00c2655a-dfec-4aa6-a334-c08f03322136.

21. On March 10, 2021, United States Magistrate Judge Andrea K. Johnstone authorized a warrant to search 4 Janet Lane Newton, New Hampshire, the person of RIMAS, and electronic devices believed to be used by RIMAS.

22. On March 11, 2021, members of Homeland Security Investigations conducted the aforementioned search warrant. Special Agent Shawn Serra and I made contact with RIMAS as he was leaving his work in Seabrook, New Hampshire. During a search of RIMAS's person, an iPhone 8 was located in his front right pocket. I proceeded to call the number I had been communicating with on WhatsApp, 978-330-6022, and the phone began to ring while displaying "Text Now Audio Call" listing my undercover number as the one calling. After observing this information, I placed the phone in airplane mode and secured it as evidence.

23. SA Serra and I informed RIMAS we were conducting an investigation involving him and asked if he would go to the Seabrook Police Department to further speak with us. RIMAS voluntarily agreed to respond to the Seabrook Police Department and was transported there by Seabrook Detectives. At approximately 2:54 p.m., SA Serra and I began an audio/video recorded interview with RIMAS and read him his *Miranda* Rights, which he waived to speak to us. During the interview RIMAS advised the cell phone seized from his pocket belongs to him and is not used by anyone else. RIMAS has had the phone for a couple years, it is password protected, and he is the only one who knows the password. At approximately 3:09 p.m., RIMAS invoked his right to counsel and the interview concluded. During the interview RIMAS would not provide the passcode for his phone and we attempted to use his fingerprint to access the phone but were unable to.

24. Using a forensic device called GreyKey I began an extraction of the iPhone 8. GreyKey was able to successfully complete an instant AFU extraction which contained approximately 50GB of data. In the following days, I began to review the extraction by placing it into Cellebrite Physical Analyzer ("PA"). Using this tool, I selected the feature which identifies potential child sexual abuse material and nudity within images and videos. The results of this showed 7,228 potential photos which contained nudity and 5,982 which were suspected child sexual abuse material. Within the videos folder PA identified 286 videos potentially containing nudity and did not classify any potential child sexual abuse material videos.

25. I observed that the Kik application was downloaded on the phone and the Kik user whatthefckk was the Kik account associated with the phone. In the Kik application there were three videos which I believe qualify as child pornography which were not deleted and still present in a Kik chat (unknown group name). The account whatthefckk was the owner/administrator of this group chat. I was able to identify whatthefckk as the administrator or owner by reviewing the

chats within the group which were from December 15, 2020 to March 11, 2021. While doing so, I observed whatthefckk was able to remove individuals from the group, which through my knowledge of Kik messenger I know to be a feature only an administrator or owner can do. The three child sexual abuse material videos which are present in the chat are described as:

Filename: 1f6d8b5e-05a5-483b-969c-73c77419e91a
Sent by KIK user Cazzone99 on 03/09/2021 at 7:21:51 PM (UTC-5)
Description: One-minute video of a prepubescent female lying on her side wearing a pink skirt which is pulled up. An adult female has a foreign object on her pointer finger and is repeatedly inserting her finger into the female's anus. Approximately twenty seconds into the video the adult female removes the object from her finger and uses her hands to spread the prepubescent female's buttocks as the camera zooms in making the focal point the prepubescent females anus. The video next transitions a close up of the adult female rubbing and spreading the prepubescent female's vagina. In identifying the female in the video as prepubescent I based this off the females lack of breast development, bone structure, and lack of pubic hair.

Filename: b18c3cbc-dc53-4033-afd2-0c3135afb74c
Sent by KIK user Cazzone99 on 03/09/2021 at 7:29:08 PM (UTC -5)
Description: Forty-six second video of a prepubescent female in a bathtub completely naked along with another unidentifiable child. At the video starts the camera zooms in and eventually shows a close up of the female's vagina. As the video continues the female places her legs behind her head and the other unidentified child begins to rubbing/inserting her foot on the female's vagina/anus. In identifying the female in the video as prepubescent I based this off the females lack of breast development, bone structure, and lack of pubic hair.

Filename: 8c94acc0-b391-4688-a8a0-f691c4da272b.mp4
Sent by KIK user Cazzone99 on 03/02/2021 at 6:28:48 PM (UTC -5)
Description: Forty-four second video of a prepubescent female lying on her back. The video only captures the female from the belly bottom to her upper thighs. During the entirety of the video a male genitalia is being inserted/rubbed on the female's vagina. In identifying the female in the video as prepubescent I based this off the female's lack of pubic hair, bone structure, and size of her hands compared to that of the male's.

26. There were also seven files (five images and two videos) I observed which qualified as child sexual abuse material, which were either embedded or temporary files and no longer visible in the physical KIK chats. While reviewing the chats it appears that the seven files were all at one

time present in the aforementioned KIK group and you can see the date/time they were sent and individuals within the chat make comments about the pictures. The seven files are described as:

Filename: 269120a0-4287-4114-a093-43c0334f142d_embedded_1.jpg
Sent by KIK user Cazzone99 on December 15, 2020 at 7:15:16 AM (UTC -5)
Description: Digital image of a prepubescent female wearing a pink shirt. The female has her left hand on a male genitalia and has a portion of the genitalia in her mouth. In identifying the female in the video as prepubescent I based this off the female's bone structure, facial features, and size of her hands.

Filename: 49541e62-52f3-4968-8ac9-8a691d28916f_embedded_1.jpg
Sent by KIK user Cazzone99 on December 20, 2020 at 2:40:27 PM (UTC -5)
Description: Digital image of a prepubescent female lying naked on her back. An adult female wearing a mask and costume gloves is appearing to perform oral sex on the prepubescent female. In identifying the female in the video as prepubescent I based this off the female's bone structure, facial features, and lack of breast development.

Filename: 9c7d19ad-73e9-4d2d-a7aa-59ac3b08f7b0_embedded_1.jpg
Sent by KIK user Cazzone99 on December 15, 2020 at 7:15:09 AM (UTC -5)
Description: Digital image of a prepubescent female lying on her back completely naked. The angle of the image is from the area of the female's vagina/anus. The female is inserting a foreign object into her anus with her right hand. In identifying the female in the video as prepubescent I based this off the female's bone structure, lack of breast development, and lack of pubic hair.

Filename: cd6d28e0-38a4-4986-bb93-16944b19aa38_embedded_1.jpg
Sent by KIK user Warri Kempton on March 02, 2021 at 2:17:12 PM (UTC -5)
Description: Digital image of an adult female, adult male, and prepubescent female. The adult female is kissing the prepubescent female on the mouth while holding the male's erect genitalia. The prepubescent female is in the middle of the adults and has a white liquid substance on her face. In identifying the female in the video as prepubescent I based this off the female's bone structure, lack of breast development, and height.

Filename: ff6fbb6b-61f0-4a97-b626-5ac6c6eb4f43_embedded_1.jpg
Sent by KIK user Cazzone99 on February 21, 2021 at 1:21:06 PM (UTC -5)
Description: Digital image of a prepubescent female lying naked on her back. An adult female wearing a mask and costume gloves is appearing to perform oral sex on the prepubescent female. In identifying the female in the video as prepubescent I based this off the female's bone structure, facial features, and lack of breast development.

Filename: 9c7d19ad-73e9-4d2d-a7aa-59ac3b08f7b0.mp4
Sent by KIK user Cazzone99 on December 15, 2020 at 7:15:09 AM (UTC -5)
Description: Twenty-seven second video of a naked prepubescent female lying on her back. The video starts with a close up view of the female's vagina/anus and pans to show the

females chest and face. During the entirety of the video the female is inserting a foreign object into her anus using her right hand as the camera pans to different angles. In identifying the female in the video as prepubescent I based this off the female's bone structure, lack of breast development, facial features, and lack of pubic hair.

Filename: 23555e92-e730-4d80-9c29-6e5829d75579.mp4
Sent by KIK user Cazzone99 on February 23, 2021 at 6:16:58 AM (UTC -5)
Description: Fifty-three second video of a prepubescent female wearing a shirt and performing oral sex on a male genitalia. At the conclusion of the video the male ejaculates into the female's mouth. In identifying the female in the video as prepubescent I based this off the female's bone structure, lack of breast development, facial features, and size of her hands in comparison to the male.

27. Additional information of investigative interest within this chat included the following. On December 31, 2020, at 6:45:16 p.m. (UTC-5) KIK user Adam W sent the following MEGA link: https://mega.nz/folder/0RR3laJD#2hG2VpU2MPRxAuQSKvJBhg. I proceeded to copy the MEGA link into my browser in an attempt to view the contents and observed a message from MEGA indicating the link had violated their terms of service as the folder/file was reported to contain objectionable content, such as Child Exploitation Material, Violent Extremism, or Bestiality.

28. On January 05, 2021 at 2:50:49 AM (UTC -5) the KIK user Ashley Bens posted the following message "Young Trade pm."

29. Also on January 05, 2021 at 3:54:00 AM (UTC-5) the KIK user Ty Connors posted the following message "Young links?"

30. On January 10, 2021 at 1:16:13 AM (UTC -5) the KIK user Ty Connors posted the following message "Young videos."

31. On January 12, 2021 at 3:49:01 PM (UTC-5) the KIK user T Rade posted the following message "Yng Trade."

32. On January 22, 2021 at 2:18:15 PM (UTC -5) the KIK user Jal Hauj posted the following message "Trade very young @jal8551."

33. On February 17, 2021 at 4:37:16 AM (UTC -5) the KIK user Ham Burger posted the following message "Any one have any young?"

34. Also on February 17, 2021 at 5:30:38 AM (UTC -5) the KIK user Ty Connors posted the following message "Young links to trade... send to receive."

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. The evidence believed to be located within the Kik account is listed in Attachment B, which is incorporated by reference as if fully set forth herein, and is believed to be contained on servers and digital storage media maintained by and under the control of MediaLab, Inc., which owns and manages records for Kik. I request authority to search for and seize such material.

36. This application seeks a warrant to search all responsive records and information under the control of MediaLab, Inc., a provider subject to the jurisdiction of this court, regardless of where MediaLab has chosen to store such information.[4] The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within MediaLab's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

[4] It is possible that MediaLab, Inc. stores some portion of the information sought outside of the United States. Under the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), the Stored Communications Act was amended to require that communications providers in the United States respond to legal process and return relevant data regardless of the location of the servers containing the data.

37. Pursuant to 18 U.S.C. § 2703(g), this application and affidavit for a search warrant seeks authorization to require MediaLab and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to MediaLab with direction that they identify the account described in Attachment A to this affidavit, as well as other subscriber and log records associated with the account, as set forth in Section I of Attachments B to this affidavit. The search warrant will direct MediaLab to create an exact copy of the specified account and records.

38. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachments B for seizure.

39. Analyzing the data contained in the forensic copy may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic

analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachments B to the warrant.

40. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of Kik messages and documents that identify any users of the SUBJECT ACCOUNT and messages sent or received in temporal proximity to incriminating messages that provide context to the incriminating communications.

CONCLUSION

41. Based on the forgoing, I request that the Court issue the proposed search warrant authorizing a search of the SUBJECT ACCOUNT specified in Attachment A for the items more fully described in Attachment B.

Dated: April 9, 2021

Respectfully Submitted,

/s/ Adam Rayho
Adam Rayho
Task Force Officer
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire
Dated: April 9, 2021

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Kik account "whatthefckk" (display name: J J) (the "SUBJECT ACCOUNT"), that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a company based in Santa Monica, California.

Notwithstanding Title 18, United States Code, Section 2252A or similar statute or code, MediaLab shall disclose responsive data, if any, by delivering encrypted files to the United States Attorney's Office, District of New Hampshire, c/o AUSA Georgiana MacDonald, 53 Pleasant Street, 4th Floor, Concord, New Hampshire 03301.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MediaLab, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, Inc. (hereinafter "the Provider"), regardless of whether such information is stored, held or maintained inside or outside of the United States, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on or about March 04, 2021 (reference ID #00c2655a-dfec-4aa6-a334-c08f03322136), the Provider is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A, from account creation through March 11, 2021:

a. All basic subscriber information including, but not limited to:

1. Kik username;
2. Email address, birthdate, and IP address used to register the account;
3. Current email address;
4. Phone number;
5. Device related information;
6. Display name;
7. Link to most current profile picture or background;
8. Kik account creation date and IP address; and
9. Timestamp and IP address of account logins and logouts;

b. All IP addresses associated with the SUBJECT ACCOUNT;

c. All transactional chat logs associated with the SUBJECT ACCOUNT;

d. Images and videos associated with the SUBJECT ACCOUNT including unknown usernames and IP address associated with the sender/recipients of the images and videos;

e. A date-stamped log showing the usernames that the SUBJECT ACCOUNT added and/or blocked from account;

f. All abuse reports associated to the SUBJECT ACCOUNT including unknown usernames;

g. All messages and emails sent to or from the SUBJECT ACCOUNT;

h. Any information relating to groups the SUBJECT ACCOUNT belonged to from account creation to March 11, 2021, including but not limited to:

1. Group create log including the creator's username and IP address;
2. Group join logs including the inviter and invitee usernames and IO addresses;
3. Group leave logs including the remover and removed username(s) and IP addresses;
4. Group transactional chat logs including senders IP addresses;
5. Images and videos sent to the group including the sender's and receiver's usernames, and IP address associated to the sender of the images and videos; and
6. Abuse reports including all usernames;

i. All privacy settings and other account settings, including for individual Kik posts and activities;

j. All records pertaining to communications between Kik and any person regarding the user or the user's Kik account, including contacts with support services and records of actions taken.

MediaLab is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 2251(a) (sexual exploitation of minors), 18 U.S.C. § 2252(a)(2) (distribution of child pornography), 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography) those violations found in the SUBJECT ACCOUNT listed on Attachment A, including the following:

a. Information constituting evidence of production, distribution, storage, or solicitation of sexually explicit images or videos of minors;

b. Information constituting evidence of chat threads of a sexual nature relating to minors between the SUBJECT ACCOUNT and other Kik users;

c. Information constituting evidence indicating how and when the Kik accounts were accessed or used to determine the chronological and geographic context of account access, use, and events relating to the crimes under investigation and to the Kik account owner;

d. Information constituting evidence indicating the Kik account owner's state of mind as it relates to the crimes under investigation;

e. Information constituting evidence of the identity of the person(s) who created or used the Kik accounts, including records that help reveal the whereabouts of such person(s); and

f. Information constituting evidence of the identity of any person(s) who communicated with the Kik accounts about matters relating to the crimes under investigation.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct.

I am employed by Kik, Inc. ("Kik"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Kik.

The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Kik, and they were made by Kik as a regular practice; and

b. such records were generated by Kik's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Kik in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Kik, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date:_____ Signature:_____